

## Federal Trade Commission

## § 318.5

health records or PHR related entities subject to this Part.

(c) *Breaches treated as discovered.* A breach of security shall be treated as discovered as of the first day on which such breach is known or reasonably should have been known to the vendor of personal health records, PHR related entity, or third party service provider, respectively. Such vendor, entity, or third party service provider shall be deemed to have knowledge of a breach if such breach is known, or reasonably should have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider.

### § 318.4 Timeliness of notification.

(a) *In general.* Except as provided in paragraph (c) of this section and § 318.5(c), all notifications required under §§ 318.3(a)(1), 318.3(b), and 318.5(b) shall be sent without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.

(b) *Burden of proof.* The vendor of personal health records, PHR related entity, and third party service provider involved shall have the burden of demonstrating that all notifications were made as required under this Part, including evidence demonstrating the necessity of any delay.

(c) *Law enforcement exception.* If a law enforcement official determines that a notification, notice, or posting required under this Part would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed. This paragraph shall be implemented in the same manner as provided under 45 CFR 164.528(a)(2), in the case of a disclosure covered under such section.

### § 318.5 Methods of notice.

(a) *Individual notice.* A vendor of personal health records or PHR related entity that discovers a breach of security shall provide notice of such breach to an individual promptly, as described in § 318.4, and in the following form:

(1) Written notice, by first-class mail to the individual at the last known address of the individual, or by email, if

the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice. If the individual is deceased, the vendor of personal health records or PHR related entity that discovered the breach must provide such notice to the next of kin of the individual if the individual had provided contact information for his or her next of kin, along with authorization to contact them. The notice may be provided in one or more mailings as information is available.

(2) If, after making reasonable efforts to contact all individuals to whom notice is required under § 318.3(a), through the means provided in paragraph (a)(1) of this section, the vendor of personal health records or PHR related entity finds that contact information for ten or more individuals is insufficient or out-of-date, the vendor of personal health records or PHR related entity shall provide substitute notice, which shall be reasonably calculated to reach the individuals affected by the breach, in the following form:

(i) Through a conspicuous posting for a period of 90 days on the home page of its Web site; or

(ii) In major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting shall include a toll-free phone number, which shall remain active for at least 90 days, where an individual can learn whether or not the individual's unsecured PHR identifiable health information may be included in the breach.

(3) In any case deemed by the vendor of personal health records or PHR related entity to require urgency because of possible imminent misuse of unsecured PHR identifiable health information, that entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (a)(1) of this section.

(b) *Notice to media.* A vendor of personal health records or PHR related entity shall provide notice to prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security, if the unsecured